Protecting shared information in networks: a network security game with strategic attacks

Bram de Witte, Paolo Frasca, Bastiaan Overvest, Judith Timmer

Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

ARTICLE TYPE

Protecting shared information in networks: a network security game with strategic attacks

Bram de Witte[1] | Paolo Frasca[2,1] | Bastiaan Overvest[3] | Judith Timmer[1]

[1]Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, 7500 AE Enschede, The Netherlands

[2]Univ. Grenoble Alpes, CNRS, Inria, Grenoble INP, GIPSA-lab, F-38000 Grenoble, France

[3]CPB Netherlands Bureau for Economic Policy Analysis, The Hague, The Netherlands

Correspondence

*Corresponding author P. Frasca. Email: paolo.frasca@gipsa-lab.fr

Summary

A digital security breach, by which confidential information is leaked, does not only affect the agent whose system is infiltrated, but is also detrimental to other agents socially connected to the infiltrated system. Although it has been argued that these externalities create incentives to under-invest in security, this presumption is challenged by the possibility of strategic adversaries that attack the least protected agents. In this paper we study a new model of security games in which agents share tokens of sensitive information in a network of contacts. The agents have the opportunity to invest in security to protect against an attack that can be either strategically or randomly targeted. We show that, in the presence of random attack, under-investments always prevail at the Nash equilibrium in comparison with the social optimum. Instead, when the attack is strategic, either under-investments or over-investments are possible, depending on the network topology and on the characteristics of the process of the spreading of information. Actually, agents invest more in security than socially optimal when dependencies among agents are low (which can happen because the information network is sparsely connected or because the probability that information tokens are shared is small). These over-investments pass on to under-investments when information sharing is more likely (and therefore, when the risk brought by the attack is higher). In order to keep our analysis tractable, some of our results on strategic attacks make an assumption of homogeneity in the network, namely that the network is vertex-transitive. We complement these results with an analysis on star graphs (which are non-homogeneous), which confirms that the essential lines of our findings can remain valid on general networks.

KEYWORDS:

Security game, Privacy game, Network externalities, Large networks

1 | INTRODUCTION

Our society and economy have become largely dependent on sharing information over networks. Although in general computer networks provide benefits, they are also prone to cyber attacks, whose impact increases with our dependence on them. Security breaches can have various origins, such as the spread of malware, compromissions of social network accounts, or exploitations of system vulnerabilities. In this paper, we interested in cyber attacks where, without permission, confidential information is obtained. This information may represent for instance confidential documents, intellectual property or identity information. The

impact of having sensitive information stolen can be destructive: bank accounts can be plundered, companies can be threatened that strategic decisions or sensitive information will be released or identities can be stolen for criminal purposes. These forms of cyber attacks where confidential information is obtained are occurring more often and keeping personal information out of the hands of thieves is becoming increasingly difficult[1].

From both the scientific literature and the general media[2], it is apparent that the variety of potential threats is huge. Depending on their purpose, some attacks aim at compromising a whole class of systems or devices, whereas others aim at precise targets. We shall refer to the former type of attacks as random attacks and to the latter type as strategic attacks[3,4]. An example of a random cyber attack would be WannaCry. This is a ransomware virus that in 2017 infected about 200,000 computers worldwide, including computers of the National Health Service in the UK, Renault in France and Telefonica in Spain: these computers were all vulnerable because their operators failed to install in time a simple software patch - i.e. arguably under-invested in security measures. Examples of strategic cyber attacks are quite common. A well-known attack is the 2016 security breach against the Democratic National Committee, by which thousands of e-mails were stolen and subsequently leaked, including e-mails from Hillary Clinton. Other examples of strategic attacks are Distributed Denial-of-Service (DDoS) attacks that are aimed against specific websites. In April 2013 a number of websites of Dutch banks became unreachable for legitimate users[5]. These attacks were temporary and did not seem to have had a direct financial impact on bank account holders, but the banks' perceived loss of reputation was significant. Mostly to prevent additional reputation losses[6], banks invested heavily in the prevention and mitigation of DDoS-attacks, with the result that for several years no significant DDoS-attack against banks was successful: from a purely financial perspective, these investments might have been excessive.

Researchers have soon recognized that network security is not only a matter of devising suitable security measures, but also of making sure that individuals put them into practice[2]. Consequently, the adoption of security measures has been regarded as an economic problem and has been addressed with the tools of game theory. In this perspective, the key observation is that the presence of a network introduces interdependencies between risks and costs incurred by the individuals[7]. Hence, the interesting question becomes understanding the effects of these interdependencies. In order to answer this question, a large literature has been developed not only in the economic science but also in computer science[4] and in engineering, including security problems for wireless communication[8] and interdependent control systems by[9,10,11,12]. These works have addressed an array of questions that are relevant in our own work, including security games featuring strategic attacks[13], multiple targets[4], multiple attackers and defenders[14]. In this Introduction, we will not try to provide a complete literature survey on interdependent security, for which we can point the reader to sources like[15,16,17,18]. Instead, we will more modestly highlight a few recurring issues that motivate our work on interdependencies in network security.

A number of papers[15,19] have argued that security investments are not as high as they should be due to *externalities* in the network. These externalities originate because confidential information can be leaked through other channels than one's own device. As a consequence, agents face risks whose magnitude depend not only on their own security levels but also on the security levels of others. In this setting, investments act like *strategic complements* as benefits of security adoption are not exclusively for the one that invested in the security. Consequently, a negligent agent who does not adequately protect her and others' information due to free-riding, may cause considerable damage to other agents in the network. This leads to situations where benefits of security adoption might fall significantly below the cost of adoption, which causes under-investments.

More recently, the prediction of under-investments in information networks has been challenged. Acemoglu *et al.*[3] and Bachrach *et al.*[20] show that investments in security might as well be *strategic substitutes* when agents face an intelligent threat. In their setting, an attacker can aim at the weakest nodes: in this case, a negligent agent who does not invest in security has a relative higher chance that her information is stolen by a direct attack of the hacker. This eliminates the ability to free-ride on security investments of others and forces an agent to invest. In fact, this framework leads to incentives which correspond to an arms race: agents compete with each other leading to over-investments in security. Bachrach *et al.* even propose that an optimal policy requires taxing security, contrarily to subsidizing security as recommended by models that do not include an intelligent adversary.

Our work provides a tractable model of network security game that can explain both under-investments and over-investments, depending on the strategy of attack and on the amount of shared information, which eventually depends on the topology of the network connecting the agents. Our original framework and our results can be informally described as follows. Inspired by attacks that aim at recovering sensitive information, such as the DNC hack, we define a dissemination model where interconnected agents share confidential information (e-mails) with each other with a certain probability p, resulting in a dissemination of information among peers that depends on the network structure. Agents store information (both their own and that received from others) and invest in security to protect it. A malignant and possibly intelligent attacker, who has the goal to obtain as

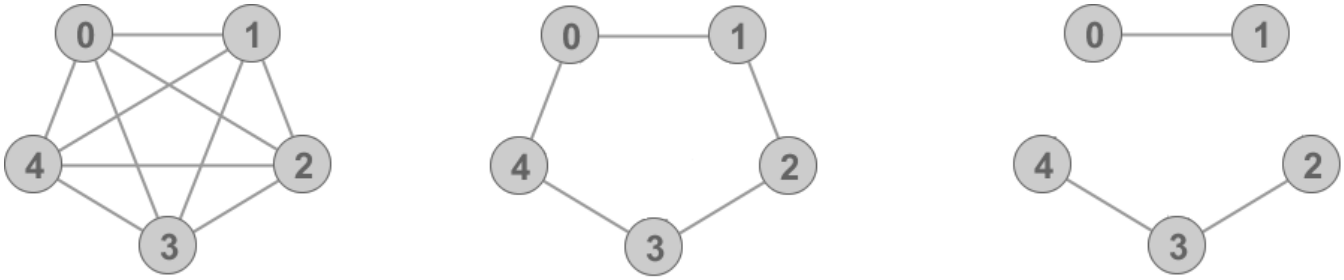

FIGURE 1 The leftmost network is a complete network and the middle one is a ring network. In the ring, $\{(0,1)(1,2)(2,3)\}$ is a possible path from agent 0 to agent 3. As each edge in the ring is also in the complete network, the ring is a subnetwork of the complete network. While the rightmost network is not connected, it is a subnetwork of the ring and of the complete network.

much information as possible, attacks one of the agents. If the attack is successful, the attacker acquires all the information that was stored by the agent, thus making this agent and possibly also other agents, which have entrusted their information to the attacked agent, victims of the attack. If the attacker is able to optimally choose which agent to attack, the attack will be said to be *strategic*: otherwise, to be *random*. In our model, the security investments are the outcome of the resulting two-stage game between the agents and the attacker, where the attacker knows the investments of the agents, who in turn choose their investments anticipating the strategy of the attacker. Under this game structure, we show that when the attack is random, then the equilibrium investments are lower than the socially optimal investments. Instead, if the attack is strategic, then the relation between optimal and equilibrium investments depends on the amount of information shared: when the fraction of shared information is low, equilibrium investments are higher than optimal ones, whereas the opposite happens when the fraction of shared information is high. The fraction of shared information can be high for two distinct reasons: either the diffusion probability p is high, or the network is tightly connected. The latter case shows our results to be consistent with those in[13], where the authors adapt interdependent security games to model strategic attacks and find thatï£¡ï£¡ over-investments prevail in nondense networks.

In order to keep our analysis tractable, some of our results on strategic attacks make an assumption of homogeneity in the network, namely that the network is vertex-transitive. We complement these results with an analysis of the security game on star graphs, which we choose as a natural example of non-homogeneous topology: this case study shows that the essential lines of our findings, as we described them above, can remain valid for other network structures.

This paper is structured as follows. Section 2 describes the problem that we want to address, introducing the dissemination model, the attack and the security investments. Subsequently, Section 3 examines the dissemination model that underlies the security game. Sections 4 and 5 are the core of our paper, as they study the security game when the attack is random and when the attack is strategic, respectively. Finally, Section 6 discusses the obtained results and complements them with numerical evaluations on complete, ring, and star graphs that we have selected as fundamental examples. Section 7 summarizes and concludes the paper. The body of the paper is complemented by an Appendix which is devoted to detailed derivations (for the examples of complete and star graphs) and proofs (of the main results about strategic attacks).

2 | INFORMATION DISSEMINATION AND NETWORK GAME

Our dynamics of interest take place on a network of agents that can share tokens of information, such as confidential documents, with each other. Let us think of n agents in a set $V = \{1, \dots, n\}$. We say that two agents i and j are linked by an edge (i, j) when i and j can share documents directly with each other. These edges create a (undirected) network $\mathcal{G} = \langle V, A \rangle$, where $A : V \times V \to \{0, 1\}$ is the adjacency matrix in which $A(i, j) = A(j, i) = 1$ if and only if i and j are linked by an edge. We denote the set of all edges in $\mathcal{G}$ as $E(\mathcal{G})$. In this graph theoretical context, we need to recall some standard definitions. A path u in $\mathcal{G}$ between agent i and j is a sequence of distinct edges $u = \{(i, \kappa_1), (\kappa_1, \kappa_2), \dots, (\kappa_{\ell-1}, \kappa_\ell), (\kappa_\ell, j)\}$, where $|u| = \ell$ is the length of the path. We assume that $\mathcal{G}$ is a network in which there exists a path between all pairs of agents, in other words, $\mathcal{G}$ is a connected network. A subnetwork $\mathcal{G}' = (V', A')$ of $\mathcal{G}$ is a network such that $V' \subset V$ and $E(\mathcal{G}') \subset E(\mathcal{G})$. In Figure 1 we illustrate these concepts and show some networks of interest.

Our problem statement requires us to specify three key ingredients: (i) the dissemination of information, (ii) the adversary attack, (iii) the defensive investments.

Information dissemination model.

We assume that initially every agent owns a unique document which we will denote as d_i for agent i. All the n documents spread, independently of each other, over the network $\mathcal{G}$. Although the documents are confidential, it is not detrimental for an agent when her document is obtained by other agents. We assume that an agent obtains a document from another agent with probability p when they are connected. This leads to a so-called *transmission network* for each document. A generic transmission network $\mathcal{T}$ is a random subnetwork of $\mathcal{G}$ and formally defined as $\langle V, \tilde{A} \rangle$, where

$$\tilde{A}(i,j) = \tilde{A}(j,i) = X_{ij}\ A(i,j)$$

where X_{ij} are independent random variables identically distributed according to a Bernoulli distribution with parameter p. We are thus assuming that the probability of transmission between two neighboring nodes is identical for every document. Let $\mathcal{T}_\ell$ and $x_{ij,\ell}$ be instances of transmission networks and transmission probabilities for a dissemination starting from any $\ell \in V$. Then $\mathcal{T}_\ell = \langle V, \tilde{A}_\ell \rangle$ with $\tilde{A}_\ell(i,j) = \tilde{A}_\ell(j,i) = X_{ij,\ell}\ A(i,j)$. Now, an agent obtains document d_ℓ when she is connected to agent ℓ in the transmission network $\mathcal{T}_\ell$. The spread of the n documents then is described by the n transmission networks.

The network structure determines the probability that a document spreads from its owner to another agent. We define the matrix P with elements P_{ij} representing the probability that agent j owns document d_i after dissemination

$$\begin{aligned} P_{ij} &= \Pr\{\text{there exists a path between } i \text{ and } j \text{ in } \mathcal{T}_i\} && (1)\\ &= \Pr\{\bigcup_{u \in U_{i,j}(\mathcal{G})} \{u \in U_{i,j}(\mathcal{T}_i)\}\}, && (2)\end{aligned}$$

where $U_{i,j}(\mathcal{G})$ is the set of all paths between agent i and j in network $\mathcal{G}$. Note that the matrix P is symmetric and only depends on $\mathcal{G}$ and on p. Since we assumed that $\mathcal{G}$ is connected, P contains only strictly positive elements. Although $P_{ij} = P_{ji}$, the event that j obtains d_i is independent of i obtaining d_j, because they are respectively taking place on the transmission networks $\mathcal{T}_i$ and $\mathcal{T}_j$. Denote the expected number of documents obtained by agent i as D_i and note that

$$D_i = \sum_{j \in V} P_{ji} = \sum_{j \neq i} P_{ji} + 1. \tag{3}$$

We additionally denote $\mathbf{D} = \{D_1, \ldots, D_n\}$.

Attack model.

After the documents have spread through the network, the adversary attacks one agent. We model this attack by a random variable from a distribution over the agents. This distribution is conveniently represented by the probability vector $\mathbf{a} = \{a_1, \ldots, a_n\}$ which we call *the attack vector*. When an attack on an agent is successful the attacker will steal all the documents stored at the target. This always includes an agent's own document, but may additionally include documents of other agents. We assume that the attack vector is established before the documents spread through the network.

Defense model.

Before the attack vector is chosen, agents have the opportunity to precautionary invest in security. We denote these investments $\mathbf{q} = \{q_1, \ldots, q_n\}$ as *the security vector*. These security investments are such that an attack on agent i is successful with probability $1 - q_i$. Let $x_i = 1$ denote the event that the attacker obtains document d_i, and $x_i = 0$ otherwise. Consequently, by conditioning and exploiting independence we establish that

$$\Pr\{x_i = 1\} = \sum_{j \in V} a_j (1 - q_j) P_{ij}. \tag{4}$$

Recognize that the security of an agent i, that is, the privacy of her information d_i, does not only depend on her own investment, but also depends on the investments by the other agents. Furthermore, let $|\mathbf{x}| = \sum_{i \in V} x_i$. Observe that the expected number of stolen documents is

$$\begin{aligned} \mathbb{E}(|\mathbf{x}|) &= \sum_{i \in V} \Pr\{x_i = 1\} \\ &= \sum_{i \in V} \sum_{j \in V} a_j (1 - q_j) P_{ij} \\ &= \sum_{j \in V} a_j (1 - q_j) D_j, \end{aligned} \tag{5}$$

because the attacker affects only one node directly.

Problem summary.

The timing in our problem is as follows. Firstly, the agents invest in security by selecting the security vector **q**. Secondly, the attacker chooses the attack vector **a**, possibly in order to maximize her reward. Hereafter, the documents spread through the network. Finally, one agent is attacked by the attacker. Since in our model the attacker observes the security levels of all the agents, the relevant equilibrium concept is that of the Stackelberg equilibrium of the resulting two-stage game[21]: the agents first select their security levels anticipating the decision of the attacker (as they know her strategy) and the attacker optimizes her attack strategy while having knowledge of the security choices. Let us note that the proposed sequence of players actions in the Stackelberg game (first defender, then attacker) is the interesting one to study. On the contrary, the reverse sequence would be unrealistic and would trivialize the game. Should the attacker go first, then the agents would just know who is to be attacked and would simply be able to optimally protect the target node.

More on the relation with literature on contagion and security games.

The two-stage scheme of the strategic security game that we study in this paper is adopted from the work[3] on cascading failures and contagion. However, our problem statement is different because the underlying diffusion/contagion model is different. In[3], each agents is susceptible to the attack with probability $1 - q_i$ and the infection spreads from the attacked node to all nodes that are connected to it in the sub-network spanned by the susceptible nodes. Therefore, an investment in security prevents both contagion from a direct attack and contagion through the network. Instead, in our model the susceptibility is only realized at the attacked node, whereas the dissemination of information independently takes place across all edges for all pieces of information. Therefore, nodes cannot be safe from damage even if they invest maximally in security, since their private information is shared with other nodes. Another difference is the explicit presence of the variable p, the probability of diffusion: in our results the amount of over- or under-investments is dependent on the level of interdependence in the network, which is directly influenced by the network topology and by the probability p.

3 | INFORMATION DISSEMINATION

The next proposition provides more insight about the value of D_i, the expected number of documents obtained by agent i. Its proof is straightforward and therefore omitted. In order to emphasize the dependence of D_i on p and $\mathcal{G}$, we shall use the notation $D_i(p, \mathcal{G})$. The result is illustrated in Figure 3.

Proposition 1 (Monotonicities)**.** Given a network $\mathcal{G}$, $D_i(p, \mathcal{G})$ is strictly increasing in p for all i. Given two networks $\mathcal{H} \subset \mathcal{G}$, $D_i(p, \mathcal{H}) \leq D_i(p, \mathcal{G})$, provided node i belongs to both networks.

Example 1 (Star graph)**.** Consider a star graph with n nodes: node 1 is the center and the remaining $n - 1$ nodes are the leaves. Note that (with $i, j > 1$ and $i \neq j$)

$$P_{1i} = p \qquad P_{i1} = p \qquad P_{ij} = p^2.$$

Hence,

$$D_1 = (n-1)p + 1 \qquad D_i = (n-2)p^2 + 1 + p,$$

which implies that $D_1 > D_i$.

In order to make our analysis tractable, we will often assume the networks to be vertex-transitive. Although this choice limits the scope of our results, we conjecture that economic forces in vertex-transitive networks extend to a broader class of networks. Informally, a vertex-transitive network is a network which 'looks the same' at every node. More precisely, we adopt the following definition.

Definition 1 (Vertex transitivity)**.** A network $\mathcal{G}$ is vertex-transitive if and only if for any two nodes i and j there exists a mapping ϕ such that $\phi(i) = j$ while the structure of $\mathcal{G}$ is preserved: $A(\kappa_1, \kappa_2) = A(\phi(\kappa_1), \phi(\kappa_2))$ for all $\kappa_1, \kappa_2 \in V$.

The two leftmost networks in figure 2 are examples of vertex-transitive networks. While every agent in a vertex-transitive network has the same number of other agents whom she is linked to (regular network), the converse is not necessarily true. As an example, the last network in figure 2 is regular but not vertex-transitive. It is no surprise that every agent in a vertex-transitive networks obtains — in expectation — the same number of documents. We state this formally in the next proposition.

Proposition 2 (Shared documents in vertex-transitive networks)**.** In any vertex-transitive network, $D_i = D_j$ for all $i, j \in V$.

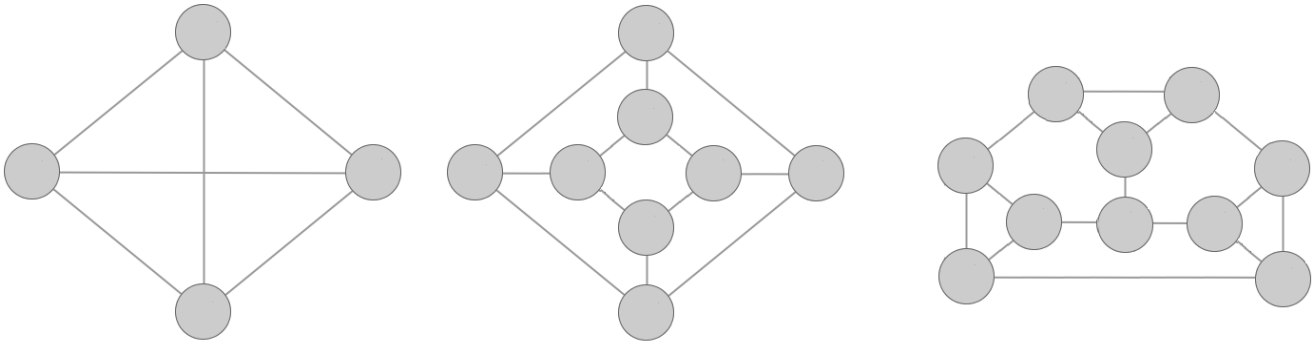

FIGURE 2 Several 3-regular networks. The complete network with 4 agents and the middle network are vertex-transitive networks. The last network is an example of a network which is regular but not vertex-transitive.

Proof. By vertex-transitivity there exists a ϕ such that $\phi(i) = j$ while the structure is preserved, which means that $P_{\ell k} = P_{\phi(\ell)\phi(k)}$. Consequently by (3), $D_i = \sum_{k\in V} P_{k,i} = \sum_{\phi(k)\in V} P_{\phi(k),j} = D_j$, yielding the result. □

Since on vertex-transitive networks all elements in $\mathbf{D}$ are identical (for all values of p), we will adopt the notation $D_i = D$. Complete graphs and ring graphs are both examples of vertex-transitive networks.

Example 2 (Ring graph)**.** Consider a ring graph with n nodes (see Figure 1). Let $\mathrm{dist}(i, j) = \min\{|i - j|, n - |i - j|\}$ be the distance between nodes i and j. By a simple inclusion-exclusion reasoning, observe that if $j \neq i$ then

$$P_{ij} = p^{\mathrm{dist}(i,j)} + p^{n-\mathrm{dist}(i,j)} - p^n.$$

Hence, by summing over the nodes

$$D = 1 + 2\sum_{\ell=1}^{n-1} p^\ell - (n-1)p^n = \frac{1 + p - p^n(n+1) + p^{n+1}(n-1)}{1-p}.$$

Note that $D \to \frac{1+p}{1-p}$ as $n \to \infty$. In contrast, recall from Example 1 that D_i is unbounded in n on star graphs.

Ring and star graphs are simple to deal with because the number of possible paths between two nodes is small. On the contrary, the complete graph has a very large number of possible connecting paths. Nevertheless, some quantities can be explicitly computed.

Example 3 (Complete graph)**.** For the sake of clarity, we denote by D^n and P^n_{ij} the expected number of documents and the generic transmission probability on the complete graph K_n, respectively. Due to transitivity,

$$D^n = 1 + (n-1)P^n_{ij}$$

and for small n we easily see that $P^2_{ij} = p$ and $P^3_{ij} = p + p^2 - p^3$. To obtain some more general expressions, let Q^n denote the probability that any document reaches all nodes in K_n. Then, $Q^1 = 1$ and

$$Q^k = 1 - \sum_{\ell=1}^{k-1} \binom{k-1}{\ell-1} (1-p)^{\ell(k-\ell)} Q^\ell. \tag{6}$$

In turn,

$$P^n_{ij} = \sum_{k=2}^{n} \binom{n-2}{k-2} (1-p)^{k(n-k)} Q^k. \tag{7}$$

These formulas, proved in the Appendix, allow for the numerical evaluation of D on graphs of moderate size, as shown in Figure 3. For large n, it is useful to consider the bounds

$$1 - (1-p)(1-p^2)^{n-2} \leq P^n_{ij} \leq 1 - (1-p)^{n-1}.$$

The lower bound can be obtained by considering only propagation across paths of length at most two. The upper bound can be obtained by considering that the document from i cannot reach vertex j unless at least one edge reaches j in graph $\mathcal{T}_i$. These two bounds together imply that D_i is asymptotically linear in n.

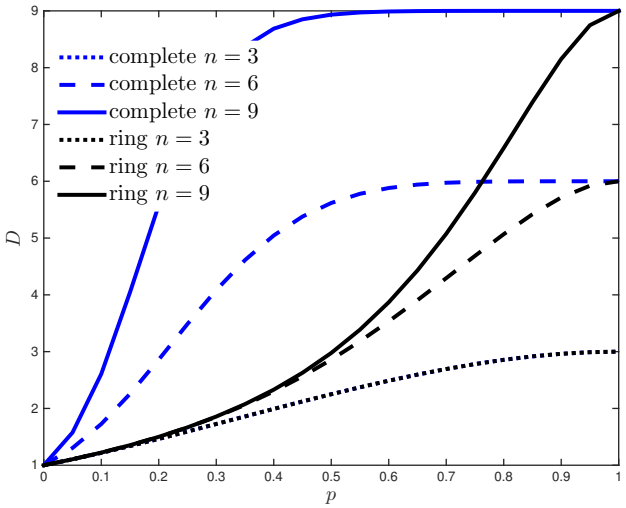

FIGURE 3 Computations on ring and complete graphs illustrate that the expected number of documents D obtained by each agent is increasing in the density of the network and in p. Note that for any graph for which the ring is a subgraph, every D_i must be higher than D in the ring and lower than D in the complete graph.

4 | SECURITY UNDER RANDOM ATTACKS

Security investments are conveniently modeled as the outcome of a game between agents. In this section, we look at the social optimum and the equilibria of this security game in the presence of a random attack. The game with a strategic attack is considered in Section 5.

The security game with random attacks is defined as follows. A random attack is defined by the uniform attack vector

$$a_i = \frac{1}{n} \quad \forall i,$$

which is known to all agents.The player set is the set of agents or nodes V. The strategy set of agent i is $Q_i = [0, 1]$. The reward of each agent i is defined as the probability that her own document is safe minus the incurred cost, that is,

$$\Pi_i = 1 - \Pr\{x_i = 1\} - c(q_i), \tag{8}$$

where $\Pr\{x_i = 1\}$ is given in (4) and $c(q_i)$ is the cost agent i incurs for choosing q_i. We assume that

$$c(q) = \frac{1}{2}\alpha q^2$$

for some $\alpha \geq 1$. The choice of a quadratic cost is made for simplicity: the analysis can be extended to other smooth convex increasing functions. The choice of α, instead, is meant to make the cost "large", so to rule out trivial game outcomes with maximal investments. Also this assumption can be relaxed at the price of more involved analysis.

In this setting each agent attempts to maximize her reward while disregarding the utilities of the others. This is described by a *noncooperative game* $(V, \{Q_i\}_{i\in V}, \{\Pi_i\}_{i\in V})$ with player set V. Any player $i \in V$ has strategy set Q_i and payoff function Π_i. For these games, the classical definition of Nash equilibrium is of interest: an investment level $\mathbf{q}^N$ is a pure strategy Nash equilibrium if for any player i and any investment level $q_i \in [0, 1]$ unilateral deviation does not pay,

$$\Pi_i(\{q_i^N, \mathbf{q}_{-i}^N\}) \geq \Pi_i(\{q_i, \mathbf{q}_{-i}^N\}).$$

Here $(\{q_i, \mathbf{q}_{-i}^N\})$ denotes the vector $\mathbf{q}^N$ where component i is replaced by q_i. In security games under random attack, the Nash equilibrium has a simple structure.

Theorem 1 (Equilibrium against random attack)**.** In a security game facing a random attack, the pure strategy Nash equilibrium $\mathbf{q}^{N,R}$ is unique and is equal to

$$q_i^{N,R} = \frac{1}{\alpha n} \quad \forall i. \tag{9}$$

Proof. The utility of agent i reads $\Pi_i = 1 - \frac{1}{n}\sum_j (1-q_j)P_{ij} - \frac{1}{2}\alpha q_i^2$. We easily see that $\frac{\partial \Pi_i}{\partial q_i} = \frac{1}{n} - \alpha q_i$ and $\frac{\partial^2 \Pi_i}{\partial q_i^2} = -\alpha < 0$. Since $\frac{\partial \Pi_i}{\partial q_i}(0, \mathbf{q}_{-i}) > 0$ and $\frac{\partial \Pi_i}{\partial q_i}(1, \mathbf{q}_{-i}) < 0$, we conclude that the largest utility is obtained with investment $q_i^{N,R} = \frac{1}{\alpha n}$, the unique only Nash equilibrium. □

Some remarks are in order. Firstly, the Nash equilibrium does not depend on p or on the network. The economic motivation for this result is intuitive. As an agent cannot control a possible external loss in a random attack, an increase in investments does not lead to a reduced risk that her document is stolen through another agent. This forces an agent — in a non-cooperative setting — to ignore the external risk and to find the optimal trade-off between investment costs and protection against a direct loss. Secondly, the investment levels at the Nash equilibrium go to zero as the number of nodes goes to infinity. This is because the risk of being attacked is diluted in large networks.

In contrast with the above non-cooperative setting, we may consider a cooperative setting where all agents cooperate to maximize the social utility, which equals the sum of the agents' utilities:

$$S(\mathbf{q}) = \sum_{i \in V} \Pi_i = n - \mathbb{E}(|\mathbf{x}|) - \sum_{i \in V} c(q_i). \tag{10}$$

By the continuity of S on its compact domain $[0,1]^n$, the function S must attain a maximum. That maximum is said to be the social optimum.

Theorem 2 (Social optimum against random attack)**.** In a network facing a random attack, the social optimum $\mathbf{q}^{O,R}$ is unique and is equal to

$$q_i^{O,R} = \frac{D_i}{\alpha n} \quad \forall i. \tag{11}$$

Proof. By (5) the global utility reads $S(\mathbf{q}) = n - \frac{1}{n}\sum_j (1-q_j)D_j - \frac{\alpha}{2}\sum_j q_j^2$. We easily see that $\frac{\partial S}{\partial q_i} = \frac{1}{n}D_i - \alpha q_i$ and

$$\frac{\partial^2 S}{\partial q_i^2} = -\alpha < 0 \qquad \frac{\partial^2 S}{\partial q_i \partial q_j} = 0,$$

implying that S is a concave function of $\mathbf{q}$. Since $\frac{\partial S}{\partial q_i}(0, \mathbf{q}_{-i}) > 0$ and $\frac{\partial S}{\partial q_i}(1, \mathbf{q}_{-i}) < 0$ because $D_i \leq n$ and $\alpha \geq 1$, we conclude that $\mathbf{q}^{O,R}$ with $q_i^{O,R} = \frac{D_i}{\alpha n}$ is the unique maximizer. □

Comparing these results shows that the Nash equilibrium features under-investments relative to the social optimum. This happens because in the cooperative setting an agent also invests to protect documents of others. This additional effort leads to higher investments in security, which depend on the network and the probability p. The following examples illustrate these observations.

Example 4 (Ring network, cont'd)**.** Consider the ring network studied in Example 2 and assume $\alpha = 1$. Then, the socially optimal investments are

$$q_i^{O,R} = \frac{1 + p - p^n(n+1) + p^{n+1}(n-1)}{(1-p)n} \quad i \in V,$$

and the Nash equilibrium investments remain $q_i^{N,R} = 1/n$. Both these quantities decrease to zero as n goes to infinity.

Example 5 (Star network, cont'd)**.** Consider the star network studied in Example 1 and assume $\alpha = 1$. Then, the socially optimal investments are

$$q_i^{O,R} = \begin{cases} \frac{(n-1)p+1}{n} & i = 1 \\ \frac{(n-2)p^2+p+1}{n} & i > 1 \end{cases}$$

Observe that all investments are non-vanishing for $n \to \infty$ and that the central node 1 supports the highest investment. On the contrary, the Nash equilibrium investments $q_i^{N,R} = 1/n$ go to zero for $n \to \infty$.

Example 6 (Complete network, cont'd)**.** Consider the complete network studied in Example 3 and assume $\alpha = 1$. Then, the socially optimal investments converge (exponentially fast in n) to the maximum investment:

$$q_i^{O,R} \to 1 \quad \text{as } n \to \infty,$$

while the equilibrium investments go to zero for $n \to \infty$.

Optimal investments are larger on networks that are well connected. Indeed, they are vanishing in the limit for large n for the cycle graph, which is poorly connected, whereas investments are non-vanishing in the limit for large n on well-connected networks such as stars and complete graphs. Consistently, the complete graph requires the highest security investments.

5 | SECURITY UNDER STRATEGIC ATTACKS

In the previous section we analysed the security game in the presence of a random attack. As of this section we allow for a strategic attack by the adversary. As such, the adversary and agents are involved in a two-stage game, the so-called *Stackelberg game*[21]. In the first stage, the agents determine their investments in security. Thereafter, in the second stage, the adversary selects an attack strategy. Such a game is solved by a Stackelberg equilibrium.

5.1 | Definition of strategic attack

We start the analysis with the strategy of the attacker. The vector $\mathbf{a}$ is chosen by the attacker in an optimal way, based on the knowledge of the network and of the vector $\mathbf{q}$. More precisely, we assume that the strategy of the attacker is an optimal trade-off between the expected number of stolen documents and the cost of this attack, solving the following optimization problem

$$\begin{aligned} \max_{\mathbf{a}} \quad & \mathbb{E}(|\mathbf{x}|) - \sum_{i \in V} \psi(a_i) \\ \text{subject to} \quad & |\mathbf{a}| = 1 \text{ and } a_i \geq 0 \text{ for all } i \in V. \end{aligned} \tag{12}$$

Here the expected number of stolen documents is $\mathbb{E}(|\mathbf{x}|)$ and the function $\psi : [0, 1] \to \mathbb{R}_{\geq 0}$ defines the cost the attacker incurs for choosing $\mathbf{a}$. Note that this framework is consistent with the attacker playing the Stackelberg game after the defending agents. In this paper we assume quadratic costs

$$\psi(a) = \frac{1}{2}\omega a^2$$

with $\omega \geq 1$. Note that this definition implies that a more precise attack is more costly than a more random one. Similarly to what was discussed for the agent's cost c, extensions to other convex increasing functions are possible. By using the expression for $\mathbb{E}(|\mathbf{x}|)$ in (5), the problem becomes

$$\begin{aligned} \max_{\mathbf{a}} \quad & \sum_{i=1}^{n} \left(a_i(1 - q_i)D_i - \frac{1}{2}\omega a_i^2 \right) \\ \text{subject to} \quad & |\mathbf{a}| = 1 \text{ and } a_i \geq 0 \text{ for all } i \in V. \end{aligned} \tag{13}$$

The Karush-Kuhn-Tucker (KKT) conditions can be used to solve (13). As the objective function is strictly concave, these conditions are necessary and sufficient to obtain the optimal solution. The KKT conditions read

$$(1 - q_i)D_i - \omega a_i + \lambda + \kappa_i = 0, \qquad \forall i, \tag{14a}$$

$$\sum_{i \in V} a_i = 1, \tag{14b}$$

$$a_i \geq 0, \qquad \forall i, \tag{14c}$$

$$\kappa_i \geq 0, \qquad \forall i, \tag{14d}$$

$$\kappa_i a_i = 0, \qquad \forall i, \tag{14e}$$

where $\lambda \in \mathbb{R}$ and $\kappa_i \in \mathbb{R}^+$ for all i are the Lagrange multipliers corresponding to the constraints (14b) and (14c) respectively. Solving these conditions results in the following characterization of the optimal attack strategy.

Proposition 3 (Optimal attack vector)**.** The optimal attack vector $\mathbf{a}^*$ chosen by the attacker, solving (13), is given by the unique solution $(\lambda^*, \mathbf{a}^*)$ to the equations

$$\omega = \sum_{i \in V} \max\{0, (1-q_i)D_i + \lambda\}, \tag{15a}$$

$$a_i = \frac{1}{\omega} \max\{0, (1-q_i)D_i + \lambda\} \quad \forall i \in V. \tag{15b}$$

Consequently, $\mathbf{a}^*$ is a function of $\mathbf{q}$ and $\mathbf{D}$ (and in turn of p and of the topology of the network).

Proof. By substituting (14a) into (14b) and noting that by (14e) $\kappa_i = 0$ if $a_i > 0$, the multiplier λ^* must solve

$$\omega = \sum_{i \in V} \max\{0, (1-q_i)D_i + \lambda\}$$

To show that λ^* is unique, suppose that there are two solutions of (15a): λ_1 and λ_2. Without loss of generality, assume that $\lambda_1 < \lambda_2$ and set $V_k = \{i \in V \mid (1-q_i)D_i + \lambda_k > 0\}$ for $k = 1, 2$. Obviously, $V_1 \subseteq V_2$. Also note that

$$\begin{aligned} 0 = \omega - \omega &= \sum_{i \in V_1} \left((1-q_i)D_i + \lambda_1\right) - \sum_{i \in V_2} \left((1-q_i)D_i + \lambda_2\right) \\ &= -\sum_{i \in V_2 \setminus V_1} (1-q_i)D_i + \lambda_1 |V_1| - \lambda_2 |V_2| < 0, \end{aligned}$$

which gives us a contradiction. So, λ^* is unique. Next, (14a) directly leads to (15b) and $a_i(\mathbf{q})$ is a well-defined function of q by the uniqueness of λ^*. □

The example below illustrates the optimal strategic attack probabilities for star networks.

Example 7 (Star network, cont'd)**.** Consider the star network studied in Example 1 and, by symmetry, assume that $q_2 = \ldots = q_n$. We begin by looking for solutions to (15) such that $a_i^* > 0$ for all i. In this case, equations (15a) and (15b) become

$$\begin{aligned} 1 = \omega &= (1-q_1)D_1 + (n-1)(1-q_2)D_2 + n\lambda^*, \\ a_1^* = \omega a_1^* &= (1-q_1)D_1 + \lambda^*, \\ a_2^* = \omega a_2^* &= (1-q_2)D_2 + \lambda^*, \end{aligned}$$

and $a_k^* = a_2^*$ for $k = 3, \ldots, n$. Solving the first equation for λ^* and substituting that in the other two equations yields

$$\begin{aligned} a_1^* &= \frac{1}{n} + \frac{1}{\omega}\left(1 - \frac{1}{n}\right)\left((1-q_1)D_1 - (1-q_2)D_2\right), \\ a_2^* &= \frac{1}{n} + \frac{1}{\omega}\frac{1}{n}\left((1-q_2)D_2 - (1-q_1)D_1\right). \end{aligned}$$

Let $\Delta = (1-q_1)D_1 - (1-q_2)D_2$ and observe that Δ can be either negative or positive and its magnitude is approximately linear in n. Since $a_1^* - a_2^* = \frac{1}{\omega}\Delta$, we observe that $a_1^* > a_2^*$ when

$$\frac{1-q_1}{1-q_2} > \frac{D_2}{D_1}.$$

Let us refer to $1 - q_i$ as the "risk" taken by agent i. Since $D_2/D_1 \to p$ when $n \to \infty$, we may say that on large star networks, the center is more likely to be attacked than the leaves when the center takes more than p times the risk taken by the leaves.

When n grows larger, the gap between the two attack probabilities increases, until $a_1^* = 1$ and $a_2^* = 0$ (if $\Delta > 0$) or until $a_1^* = 0$ and $a_2^* = \frac{1}{n-1}$ (if $\Delta < 0$). The former vector is indeed the optimal solution when $\omega \leq \Delta$, whereas the latter is optimal when $\omega \leq -(n-1)\Delta$.

Since finding explicit solutions to (15) quickly becomes unfeasible on more complex graphs, we instead set to investigate qualitative properties of the optimal attack vector. In the next result, we derive how the optimal attack probabilities depend on the investment levels $\mathbf{q}$. The formulas confirm the intuition that the optimal attack probability a_i^* is decreasing in the investments q_i of agent i, and increasing in the investments q_j of agents $j \neq i$.

Proposition 4 (How attacks depend on investments)**.** The marginal changes of the optimal attack probability $a_i^* > 0$ to q_i and to q_j for agent j with $a_j^* > 0$, are respectively given by

$$\frac{\partial a_i^*}{\partial q_i} = -\frac{n^* - 1}{\omega n^*} D_i \quad \text{and} \quad \frac{\partial a_i^*}{\partial q_j} = \frac{1}{\omega n^*} D_j \tag{16}$$

where $n^* = |\{i \in V \ : \ a_i^* > 0\}|$ is the number of agents with strict positive probability of being attacked. In particular, a_i^* is nonincreasing in q_i and nondecreasing in q_j.

Proof. The marginal changes follow from the KKT-conditions in (14). First note that $\kappa_i = 0$ when $a_i^* > 0$. Consequently when we differentiate KKT-condition (14a) with respect to q_i we get

$$\begin{aligned} -D_i - \omega \frac{\partial a_i^*}{\partial q_i} + \frac{\partial \lambda}{\partial q_i} &= 0 \\ \frac{\partial a_i^*}{\partial q_i} &= -\frac{D_i}{\omega} + \frac{1}{\omega} \frac{\partial \lambda}{\partial q_i} \end{aligned} \tag{17}$$

and — similarly — when we differentiate with respect to q_j

$$\begin{aligned} -\omega \frac{\partial a_i^*}{\partial q_j} + \frac{\partial \lambda}{\partial q_j} &= 0 \\ \frac{\partial a_i^*}{\partial q_j} &= \frac{1}{\omega} \frac{\partial \lambda}{\partial q_j} \end{aligned} \tag{18}$$

Next we combine KKT-condition (14b) with the observations above. First recognize that the equation $\sum_j a_j^* = 1$ is equivalent to $\sum_{j|a_j^*>0} a_j^* = 1$. These equations imply

$$\sum_j \frac{\partial a_j^*}{\partial q_i} = 0, \tag{19a}$$

$$\sum_{j|a_j^*>0} \frac{\partial a_j^*}{\partial q_i} = 0. \tag{19b}$$

By combining (17), (18) and (19b), it follows that

$$-\frac{D_i}{\omega} + \frac{n^*}{\omega} \frac{\partial \lambda}{\partial q_i} = 0,$$

where n^* is the number of agents with strict positive probability of being attacked. By solving this expression for $\partial\lambda/\partial q_i$ and substituting the result in (17) and (18), we establish the statement. □

Proposition 4 bears further consequences for vertex-transitive networks, where each agent obtains the same number of documents in expectation, $D_i = D$. For this reason, more precise results can be obtained, including the following monotonicity property: if an agent invests more in security than another agent, then her attack probability is lower (and vice versa).

Proposition 5 (Attacks to vertex-transitive networks)**.** If the network is vertex-transitive then $a_i^* < a_j^*$ if and only if $q_i > q_j$.

Proof. Firstly, we rewrite (15a) to obtain

$$\lambda^* = \frac{\omega}{n^*} - \frac{D}{n^*} \sum_{\ell : a_\ell^* > 0} (1 - q_\ell)$$

Next if $a_i^* > 0$ then

$$\begin{aligned} a_i^* &= \frac{1}{\omega}((1 - q_i)D + \lambda) \\ &= \frac{1}{n^*} - \frac{D}{\omega}\Big(q_i - \frac{1}{n^*} \sum_{\ell : a_\ell^* > 0} q_\ell\Big) \end{aligned}$$

It is then clear that, provided $a_i^* > 0$, $a_i^* < a_j^*$ if and only if $q_i > q_j$. If instead $a_i^* = 0$, then we derive the following equivalent inequalities.

$$\begin{aligned}(1-q_i)D + \lambda^* &\leq 0\\ \lambda^* &\leq -(1-q_i)D\\ \frac{\omega}{n^*} - \frac{D}{n^*}\sum_{\ell\,:\,a_\ell^*>0}(1-q_\ell) &\leq -(1-q_i)D\\ q_i &\geq \frac{\omega}{Dn^*} + \frac{1}{n^*}\sum_{\ell\,:\,a_\ell^*>0} q_\ell.\end{aligned}$$

At the same time, $a_j^* > 0$ is equivalent to

$$\begin{aligned}0 &< \frac{1}{n^*} - \frac{D}{\omega}\Big(q_j - \frac{1}{n^*}\sum_{\ell\,:\,a_\ell^*>0} q_\ell\Big)\\ \Leftrightarrow\ q_j &< \frac{\omega}{Dn^*} + \frac{1}{n^*}\sum_{\ell\,:\,a_\ell^*>0} q_\ell.\end{aligned}$$

Thus, $0 = a_i^* < a_j^*$ is equivalent to $q_i > q_j$. □

This result immediately leads to the following implications: (a) maximal investments in security guarantee an upper bound on the attack probability; and (b) if all agents invest the same amount, then the attack vector is uniform.

Corollary 1. For vertex-transitive networks, there hold true that:

(a) if $q_i = 1$ for some i, then $a_i^* \leq 1/n$;

(b) if $q_i = \bar{q}$ for all i, then $a_i^* = 1/n$ for all i.

5.2 | Investments under strategic attacks

In stage 1 of the security game, the security investments are conveniently modeled as the outcome of a game between the agents. In this game, they take the best response $\mathbf{a}^*(\mathbf{q})$ of the adversary into account. The reward of agent i equals (cf. (8))

$$\Pi_i = 1 - \sum_j a_j^*(1-q_j)P_{ij} - \frac{1}{2}\alpha q_i^2.$$

First we analyse the cooperative case, where the social utility

$$S = \sum_i \Pi_i = n - \sum_j a_j^*(1-q_j)D_j - \frac{1}{2}\sum_i \alpha q_i^2$$

is maximized. The proof of the following result is postponed to the Appendix.

Theorem 3 (Social optimum against strategic attacks)**.** In a vertex-transitive network facing a strategic attack, the social optimum $\mathbf{q}^{O,S}$ is unique and equal to

$$q_i^{O,S} = \frac{D}{\alpha n} \qquad \forall i \in V. \tag{20}$$

Theorem 3 indicates that it is socially optimal for an agent of a vertex-transitive network to invest the same as the others. As a consequence, one may immediately verify that $\mathbf{a}_i^*(\mathbf{q}^{O,S}) = \frac{1}{n}$, that is, the socially optimal uniform investments imply a uniform attack probability. In other words, we may say that the socially optimal investments make the strategic advantage of the adversary void.

Remark 1. Uniform investments, uniform attacks and sacrificial lambs. Theorem 3 brings up the question whether uniform investments and attack probabilities are optimal in general. On this matter, we should point out that other studies on strategic attacks identified as optimal the opposite defence strategy: leaving some agents unprotected and making them sacrificial lambs[22,23]. In our setting, it appears that the uniformity of the optimal investments as per Theorem 3 is indeed a consequence of the homogeneity of the network. However, the result that optimal investments make the attack probabilities uniform may have broader scope, since we find it to be valid also on some non-homogeneous networks, which are beyond the scope of the theorem.

As an example, we show in the Appendix that on large star graphs an investment strategy that makes the attack probability uniform is better than a strategy that leaves a sacrificial lamb.

Instead, if each agent optimizes her individual reward, the following equilibrium investment levels are attained.

Theorem 4 (Equilibrium against strategic attacks)**.** In a vertex-transitive network facing a strategic attack, there is a unique pure strategy equilibrium vector of investment levels $\mathbf{q}^{N,S}$, which is symmetric and given by

$$q_i^{N,S} = \frac{(n-D)D+\omega}{(n-D)D+\alpha n\omega} \qquad \forall i \in V. \tag{21}$$

Theorem 4, whose proof is also postponed to the Appendix, shows that the first stage of the security game results in a unique and symmetric vector of investment levels. Combining this equilibrium with the outcome of the second stage, results in the Stackelberg equilibrium of our game.

Corollary 2 (Stackelberg equilibrium)**.** The security game under strategic attack has a unique Stackelberg equilibrium with investment levels $\mathbf{q}^{N,S}$ and attack vector $\mathbf{a}^*(\mathbf{q}^{N,S})$ given by (15a), (15b) and (21).

The equilibrium investments in stage 1 are a function of D, the expected number of documents obtained, which in turn depends on the transmission probability p.

Remark 2. Dependence on p. The equilibrium investments (21) are increasing in p for small p, till the point where $D = n/2$, after which they are decreasing in p. Indeed,

$$\frac{d}{dp}\big((n-D)D\big) = (n-2D)\frac{dD}{dp}$$

and thus

$$\frac{dq_i^{N,S}}{dp} = \frac{(n-2D)\frac{dD}{dp}(\alpha n-1)\omega}{\big((n-D)D+\alpha n\omega\big)^2} \tag{22}$$

In view of Proposition 1, the only root of (22) is given by $\hat{p}$ such that $D = n/2$. Further, $dq_i^{N,S}/dp > 0$ when $D < n/2$ and $dq_i^{N,S}/dp < 0$ when $D > n/2$.

Example 8 (Ring, cont'd)**.** For ring networks we derive from Example 2 that, after neglecting exponential terms, $\hat{p} \simeq 1 - \frac{4}{n+2}$: hence, as n diverges, $\hat{p}$ converges to 1. Moreover,

$$\lim_{n\to\infty} q_i^{N,S} = \frac{\frac{1+p}{1-p}}{\frac{1+p}{1-p}+\alpha\omega}.$$

This value is strictly larger than the limit social optimum $\lim_{n\to\infty} q_i^{O,S} = 0$ as seen in Example 4. We conclude that in large rings (which are sparse networks) strategic attacks lead to over-investments, $q_i^{N,S} > q_i^{O,S}$.

Example 9 (Complete, cont'd)**.** For complete networks we derive from Example 3 that, after neglecting exponential terms, $D \simeq n$ as n diverges. This implies that

$$q_i^{N,S} \simeq \frac{1}{\alpha n}.$$

Comparing this value with the limit social optimum $\lim_{n\to\infty} q_i^{O,S} = \frac{1}{\alpha}$, we conclude that in large complete graphs strategic attacks lead to under-investments.

6 | DISCUSSION

The investment levels derived in the previous sections can easily be compared. A summary of the most relevant comparisons is given in the following statement.

Theorem 5 (Investments in vertex-transitive networks)**.** Assume the graph $\mathcal{G}$ to be vertex-transitive.

1. Socially optimal investments do not depend on the type of attack, that is, $q_i^{O,R} = q_i^{O,S}$.

2. Equilibrium investments are smaller in case of random attacks than in case of strategic attacks, that is, $q_i^{N,R} \leq q_i^{N,S}$ and the inequality is strict unless $p = 1$.

3. Random attacks lead to under-investments at equilibrium, that is, $q_i^{N,R} \leq q_i^{O,R}$ and the inequality is strict unless $p = 0$.

4. Strategic attacks can lead to either under- or over-investments. The level of investment depends on the probability p: for smaller p, over-investments occur, $q_i^{N,S} > q_i^{O,S}$ and for larger p, it leads to under-investments occur, $q_i^{N,S} < q_i^{O,S}$. Moreover, the condition

$$2(n - D)D \geq (n - 2D)(\alpha n - 1) \tag{23}$$

is sufficient to guarantee a unique transmission probability p^* at which the equilibrium investments are socially optimal, $q_i^{N,S} = q_i^{O,S}$.

Proof. The first three items may be verified immediately by inspection. For the fourth item, denote the investments by $q_i(p)$ to stress the dependence on p. Observe that that $q_i^{N,S}(1) = q_i^{O,S}(0) = \frac{1}{\alpha n}$, $q_i^{O,S}(1) = \frac{1}{\alpha}$ and $q_i^{N,S}(0) > \frac{1}{\alpha n}$. This implies that the graphs of $q_i^{N,S}(p)$ and $q_i^{O,S}(p)$ intersect at least once.

Applying the chain rule of differentiation and the fact that D increases with p lead to the following inequalities:

$$\begin{aligned}
\frac{\partial}{\partial p} q_i^{O,S} &> \frac{\partial}{\partial p} q_i^{N,S} \\
\frac{\partial}{\partial D} \frac{D}{\alpha n} &> \frac{\partial}{\partial D} \left(1 - \frac{(\alpha n - 1)\omega}{(n - D)D + \alpha\omega n} \right) \\
\frac{1}{\alpha n} &> \frac{(\alpha n - 1)\omega(n - 2D)}{\left((n - D)D + \alpha\omega n\right)^2} \\
(n - D)D + (\alpha\omega n)^2 + \alpha\omega n\,(2(n - D)D - (n - 2D)(\alpha n - 1)) &> 0.
\end{aligned}$$

A sufficient condition for the latter inequality to be true is given by (23). □

A few comments about this statement are in order. Regarding social optima, the reader may find it surprising that optimal investments against random and strategic attacks coincide. Indeed, the optimal investments against strategic attacks trivialize the strategy of the attacker, that is, make the attack probabilities uniform. This observation is confirmed by the star graph example, described in the Appendix, where the investments that make the attack uniform yield higher reward than sacrificing lamb investments. In the special case of vertex-transitive networks, the uniformity in the attack probability is reflected in the uniformity of the investments.

Regarding equilibria, we observe that equilibrium investments against strategic attacks are always higher than against random attacks, which feature under-investment in comparison with the social optimum. In other words, players that are aware of the strategic nature of the attack shall invest more than against a random attack. This difference is consistent with intuition, since players facing a strategic attacker can be expected to invest more to divert attacks away from themselves. However, the theorem also shows that the awareness of strategic attacks is not sufficient to prevent under-investments (even though strategic investments remain larger than investments in the random setting). Actually, under-investments against strategic attacks appear precisely when the risk is higher, that is, in the presence of a larger transmission probability and a more tightly connected networks. Indeed, the turning point p^* from over- to under-investments is lower in denser networks.

The prevalence of over- or under-investments depends on whether positive or negative externalities prevail in the network game under strategic attacks. At low p, over-investments are due to the "arms race" to divert attacks towards other agents. At the extreme case $p = 0$, each agent is the sole responsible for the safety of her own information. On the contrary, high values of p mean that the information is widely shared and agents have ampler opportunity to free-ride the investments of others.

These facts can be numerically verified in our running examples. We report in Figures 4, 5 and 6 the optimal and equilibrium investments as functions of the diffusion probability p, computed for complete, ring, and star topologies with $n = 5$ nodes. Several observations can be made about the similarities and differences between these three very different networks (we remind that the star graph is not vertex-transitive, therefore not covered by Theorem 5).

1. On all these networks, strategic attacks make the agents invest more at equilibrium than random attacks.

2. On all these networks, the optimal strategic investments are increasing and become equal to $1/\alpha$ when $p = 1$ and equal to $\frac{1}{\alpha n}$ when $p = 0$: at that point they coincide with the equilibrium investments against random attack. Instead, equilibrium investments become equal to $\frac{1}{\alpha n}$ when $p = 1$. The extreme values for $p = 0, 1$ do not depend on the topology.

3. On all these networks, the equilibrium results in over-investments for small transmission probabilities p and in under-investments for large transmission probabilities.

4. For each node, there is a unique probability p_i^* where over-investments pass on to under-investments and equilibrium investments are socially optimal.

5. The transition from over-investments to under-investments takes place at smaller transition probabilities where connectivity is stronger. Consistently, the probability with the largest equilibrium investment level is smaller where connectivity is stronger.

These observations are consistent with our theoretical results, even if some of them were proved for vertex-transitive networks only, thereby showing that their insights may also be valid on other classes of networks.

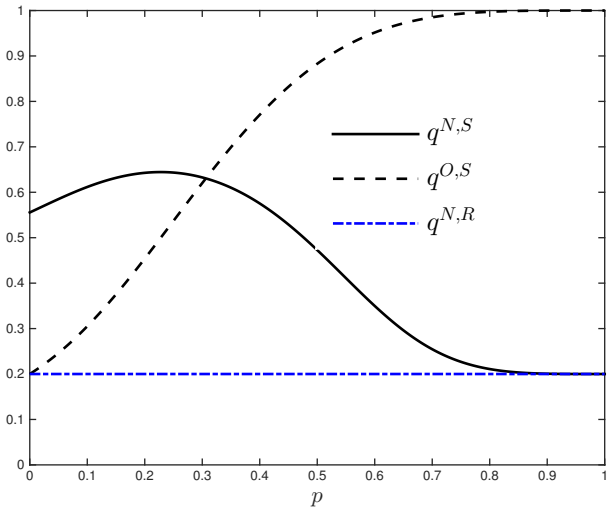

FIGURE 4 Security investments in a complete graph with $n = 5$ nodes where $\alpha = \omega = 1$.

7 | CONCLUSION

In this paper, we studied in detail a model of strategic defensive allocation to elucidate the economic forces at play. We have shown how the type of attack by the adversary influences the investments by the agents. Equilibrium investments are larger under strategic attacks than under random attacks. Furthermore, in case of random attacks the equilibrium investments are always lower than socially optimal, which represents under-investments in security. Finally, in case of strategic attacks, there are over-investments for small transmission probabilities p and under-investments for large probabilities. This transition takes place at lower probabilities p in denser networks. Indeed, those networks where the stakes are higher, because the number of shared documents is larger, are precisely those that are prone to under-investments.

In a large part of this work, the assumption of vertex-transitivity postulates a homogeneity in the network, which greatly simplifies the analysis. Another simplifying assumption is the choice of quadratic costs. Even though extending the scope of our analysis would certainly be of interest, we believe that our contribution already exemplifies the fundamental issues of these network privacy games and the key role of the network topology therein.

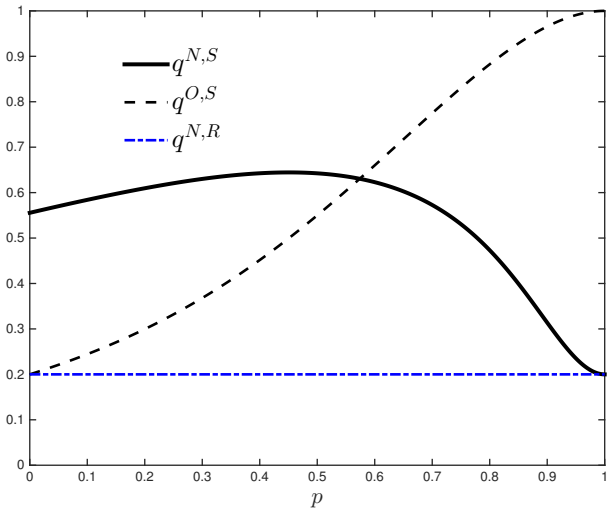

FIGURE 5 Security investments in a ring graph with $n = 5$ nodes where $\alpha = \omega = 1$.

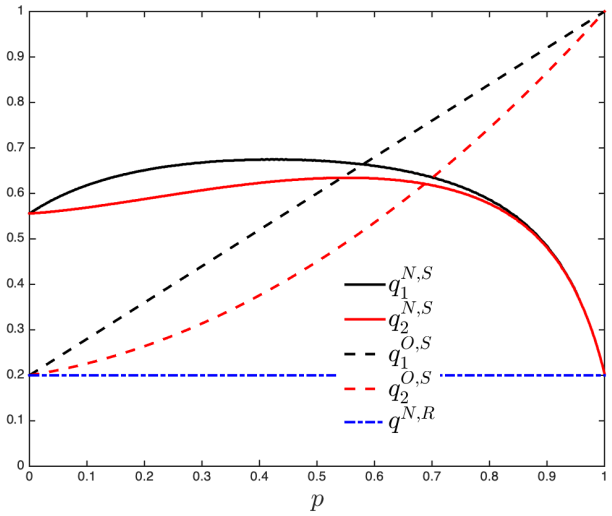

FIGURE 6 Security investments in a star graph with $n = 5$ nodes where $\alpha = \omega = 1$.

The importance of the network topology is reflected by the fact that optimal investments in random and strategic attacks and equilibrium investments in strategic attacks depend explicitly on the expected number of received documents and, therefore, on the topology. Therefore, the players need to know about the topology to implement their strategies. Since such a knowledge may be hard to obtain in practice, a relevant open question is defining a version of this security game that takes into account suitable limitations of such knowledge.

□

APPENDIX

A INFORMATION DISSEMINATION ON THE COMPLETE GRAPH

We begin by proving[1] formula (6).

Proposition 6. Let Q^n be the probability that any document reaches all nodes in K_n. Then, for any p, it holds that $Q^1 = 1$ and

$$Q^n = 1 - \sum_{\ell=1}^{n-1} \binom{n-1}{\ell-1} (1-p)^{\ell(n-\ell)} Q^\ell \qquad \forall n > 1.$$

Proof. Let $\mathcal{T}_i^n$ be a transmission network in K_n and observe that Q^n is equal to the probability that $\mathcal{T}_i^n$ is connected. Let $C_n(i)$ be the component in which i lies in the transmission network $\mathcal{T}_i^n$ and compute

$$\begin{aligned}\Pr\{\mathcal{T}_i^n \text{ is connected }\} &= \Pr\{|C_n(i)| = n\} \\ &= 1 - \sum_{\ell=1}^{n-1} \Pr\{|C_n(i)| = \ell\},\end{aligned}$$

where $|C_n(i)|$ is the number of nodes in $C_n(i)$. To evaluate $\Pr\{|C_n(i)| = \ell\}$, let $\mathcal{V}_\ell$ be the set of the subsets of V that include node i and have cardinality ℓ: recognize that there are $\binom{n-1}{\ell-1}$ such subsets. Next, by conditioning on all $\tilde{V} \in \mathcal{V}_\ell$ and exploiting the assumptions of independence between the edges, we can compute

$$\begin{aligned}\Pr\{|C_n(i)| = \ell\} &= \sum_{\tilde{V} \in \mathcal{V}_\ell} \Pr\{C_n(i) = \tilde{V}\} \\ &= \sum_{\tilde{V} \in \mathcal{V}_\ell} \Pr\{\ \tilde{V} \text{ is connected in } \mathcal{T}_i^n\ \} \Pr\{\text{ no edge between } \tilde{V} \text{ and } V \setminus \tilde{V}\ \} \\ &= \sum_{\tilde{V} \in \mathcal{V}_\ell} \Pr\{|C_\ell(i)| = \ell\} (1-p)^{\ell(n-\ell)} \\ &= \binom{n-1}{\ell-1} (1-p)^{\ell(n-\ell)} \Pr\{|C_\ell(i) = \ell|\},\end{aligned} \tag{A1}$$

so concluding the proof. □

Next, we prove Equation (7).

Proposition 7. In a complete network on n nodes, for every p and all $i \neq j$

$$P_{ij}^n = \sum_{k=2}^{n} \binom{n-2}{k-2} (1-p)^{k(n-k)} Q^k.$$

Proof. By conditioning on the size of the component in which j lies

$$\begin{aligned}P_{ij}^n &= \Pr\{j \text{ is connected to } j \text{ in } \mathcal{T}_i\} \\ &= \sum_{k=1}^{n} \Pr\{j \text{ is connected to } j \text{ in } \mathcal{T}_i |\ |C_n(j)| = k\} \Pr\{|C_n(j)| = k\} \\ &= \sum_{k=1}^{n} \frac{k-1}{n-1} \Pr\{|C_n(j)| = k\},\end{aligned}$$

where we have used the fact that all nodes are equally likely to be in $C_n(j)$. The result follows by using (A1). □

[1]The result in Proposition 6 is probably well known. For instance it can be found stated in slide 4 of http://keithbriggs.info/documents/connectivity-Manchester2004Nov19.pdf. Here we provide a proof for completeness.

B SACRIFICIAL VS UNIFORM STRATEGIES ON THE STAR GRAPH

Let us first consider the strategy that ensures uniform attack probabilities. From the derivations in Example 7, we observe that when $\Delta = 0$, necessarily $a_i^* = \frac{1}{n}$ and $q_1 = 1 - (1 - q_2)\frac{D_2}{D_1}$. Therefore,

$$\begin{aligned} S =& n - \sum_j a_j^*(1 - q_j)D_j - \frac{\alpha}{2}\sum_j q_j^2 \\ =& n - (1 - q_2)D_2 - \frac{\alpha}{2} + \alpha(1 - q_2)\frac{D_2}{D_1} - \frac{\alpha}{2}(1 - q_2)^2\frac{D_2^2}{D_1^2} - \frac{\alpha}{2}(n-1)q_2^2 \end{aligned}$$

Its derivative is

$$\frac{\partial S}{\partial q_2} = D_2 - \alpha\frac{D_2}{D_1} + \alpha\frac{D_2^2}{D_1^2} - q_2\Big(\alpha\frac{D_2^2}{D_1^2} + \alpha(n-1)\Big),$$

showing that the reward is optimal for

$$q_2 = \frac{\frac{D_2}{\alpha} - \frac{D_2}{D_1} + \frac{D_2^2}{D_1^2}}{\frac{D_2^2}{D_1^2} + n - 1}.$$

Since the expression for the resulting optimal reward is cumbersome, we prefer to present an approximation for large n. In that limit, we find

$$\frac{S^*}{n} = 1 - p^2 + \frac{p^4}{2\alpha} + O\left(\frac{1}{n}\right).$$

Moreover, notice that $q_2^* = \frac{p^2}{\alpha} + O\left(\frac{1}{n}\right)$ and $q_1^* = 1 - p + \frac{p^3}{\alpha} + O\left(\frac{1}{n}\right)$, where the latter quantity is larger than the former: the center has to invest more than the leaves to ensure uniform attacks.

Let us then compare this reward with that of a sacrificial lamb. In this strategy we assume that one of the leaves is left unprotected, $q_{\text{lamb}} = 0$. In this case, equations (15) imply that $a_{\text{lamb}} = 1$ as long as q_1 and q_2 are large enough: more precisely, as long as

$$q_2 \geq \frac{\omega}{D_2} \tag{B2a}$$

$$q_1 \geq \frac{\omega + D_1 - D_2}{D_1} \tag{B2b}$$

Note that the first lower bound goes to zero in the limit of large n, whereas the second one converges to $1 - p$: therefore, the lamb strategy is feasible. Under conditions (B2), we can calculate

$$\begin{aligned} S_{\text{lamb}} =& n - \sum_j a_j^*(1 - q_j)D_j - \frac{\alpha}{2}\sum_j q_j^2 \\ \leq& n - D_2 - \frac{\alpha}{2}\left(\left(1 - \frac{D_2}{D_1} + \frac{\omega}{D_1}\right)^2 + (n-2)\frac{\omega^2}{D_2^2}\right) \\ =& n(1 - p^2) + o(n). \end{aligned}$$

This quantity is asymptotically smaller than S^*, thereby showing that the uniform strategy gives higher reward, at least for large enough networks. Incidentally, we remark that the cost incurred to satisfy conditions (B2) becomes negligible in the limit.

C PROOF OF THEOREM 3

The proof takes four steps. (i) We show that no component of $\mathbf{q}^{O,S}$ is either 0 or 1. (ii) We deduce the first order conditions (FOC) for optimality of the social optima. (iii) We show that there is no asymmetric investment level which solves this FOC. (iv) We find a symmetric social optimum and prove that this (symmetric) optimum is unique.

(i) Preliminary, we compute the gradient of S as

$$\frac{\partial S}{\partial q_i} = -\sum_j \frac{\partial a_j^*}{\partial q_i}(1 - q_j)D_j + a_i^* D_i - \alpha q_i.$$

By the assumption of vertex-transitivity this reduces to

$$\frac{\partial S}{\partial q_i} = -D \sum_j \frac{\partial a_j^*}{\partial q_i}(1 - q_j) + a_i^* D - \alpha q_i. \tag{C3}$$

Next, we show that the gradient of S does not point outward at the boundary of $[0, 1]^n$. First,

$$\begin{aligned}\frac{\partial S}{\partial q_i}(\{q_i = 0, \mathbf{q}_{-i}\}) &= -D\frac{\partial a_i^*}{\partial q_i} - D \sum_{j \neq i} \frac{\partial a_j^*}{\partial q_i}(1 - q_j) + a_i^* D \\ &\geq -D\frac{\partial a_i^*}{\partial q_i} - D \sum_{j \neq i} \frac{\partial a_j^*}{\partial q_i} + a_i^* D \\ &= -D \sum_j \frac{\partial a_j^*}{\partial q_i} + a_i^* D = a_i^* D > 0,\end{aligned}$$

where the final equality follows from (19a). Second,

$$\begin{aligned}\frac{\partial S}{\partial q_i}(\{q_i = 1, \mathbf{q}_{-i}\}) &= -\sum_{j \neq i} \frac{\partial a_j^*}{\partial q_i}(1 - q_j)D + a_i^* D - \alpha \\ &\leq -\sum_{j \neq i} \frac{\partial a_j^*}{\partial q_i}(1 - q_j)D < 0,\end{aligned}$$

where the weak inequality follows from $a_i^* D - \alpha \leq 0$ due to $D \leq n$, $a_i^* \leq 1/n$ due to Corollary 1.(a), and $1 \leq \alpha$.

(ii) The social optimum $\mathbf{q}^{O,S}$ thus belongs to $(0, 1)^n$. From (C3) and $\partial S/\partial q_i = 0$ the social optimum solves for each agent i

$$\alpha q_i = a_i^* D - D \sum_j \frac{\partial a_j^*}{\partial q_i}(1 - q_j). \tag{C4}$$

(iii) In order to prove that all components of $\mathbf{q}^{O,S}$ are equal, without loss of generality let $q_1 = \max \mathbf{q}^{O,S}$ and $q_2 = \min \mathbf{q}^{O,S}$ and assume that $q_1 > q_2$. We derive a contradiction. Observe that by (C4)

$$\begin{aligned}\alpha q_1 &= a_1^* D - D\frac{\partial a_1^*}{\partial q_1}(1 - q_1) - D \sum_{i \neq 1} \frac{\partial a_i^*}{\partial q_1}(1 - q_i) \\ &= a_1^* D + D \sum_{i \neq 1} \frac{\partial a_i^*}{\partial q_1}(1 - q_1) - D \sum_{i \neq 1} \frac{\partial a_i^*}{\partial q_1}(1 - q_i),\end{aligned} \tag{C5}$$

where the last equality is due to (19a) for $i = 1$. Similarly

$$\begin{aligned}\alpha q_2 &= a_2^* D - D\frac{\partial a_2^*}{\partial q_2}(1 - q_2) - D \sum_{i \neq 2} \frac{\partial a_i^*}{\partial q_2}(1 - q_i) \\ &= a_2^* D + D \sum_{i \neq 2} \frac{\partial a_i^*}{\partial q_2}(1 - q_2) - D \sum_{i \neq 2} \frac{\partial a_i^*}{\partial q_2}(1 - q_i),\end{aligned} \tag{C6}$$

with the last equality due to (19a) for $i = 2$. Observe that $a_1^* < a_2^*$, the definition of q_1 implies $0 \leq 1 - q_1 \leq 1 - q_i^{O,S}$ and that $\partial a_i^*/\partial q_1 \geq 0$ for all $i \neq 1$ by (16). Then

$$D \sum_{i \neq 1} \frac{\partial a_i^*}{\partial q_1}(1 - q_1) - D \sum_{i \neq 1} \frac{\partial a_i^*}{\partial q_1}(1 - q_i) = -D \sum_{i \neq 1} \frac{\partial a_i^*}{\partial q_1}(q_1 - q_i) = \alpha q_1 - a_1^* D < 0,$$

with the final equality due to (C4) and the inequality follows from $q_1 - q_\ell > 0$ for at least one ℓ. By a similar line of arguments

$$D \sum_{i \neq 2} \frac{\partial a_i^*}{\partial q_2}(1 - q_2) - D \sum_{i \neq 2} \frac{\partial a_i^*}{\partial q_2}(1 - q_i) = \alpha q_2 - a_2^* D > 0.$$

These two inequalities prove that the right-hand side of (C6) is larger than the right-hand side of (C5), which contradicts $q_1 > q_2$. Therefore, $q_1 = q_2$ and all components of $\mathbf{q}^{O,S}$ are equal.

(iv) Now we have established that $\mathbf{q}^{O,S}$ is a symmetric social optimal investment level, we elaborate (C4) to derive $\alpha q_i^{O,S} = a_i^* D - D(1 - q_i^{O,S}) \sum_j \frac{\partial a_j^*}{\partial q_i} = a_i^* D$ by (19). By summing $q_i^{O,S} = a_i^* D/\alpha$ over all i and using symmetry we obtain (20).

D PROOF OF THEOREM 3

Notice that the agents play a strategic game amongst themselves in stage 1. We refer to the outcome of that stage as an equilibrium. The proof is divided into three intermediate steps.

1. We prove that there exists at least one pure strategy equilibrium.
2. We prove that the equilibrium is unique and symmetric.
3. We exhibit a symmetric equilibrium.

Let us preliminary recall the reward of agent i,

$$\Pi_i = 1 - \sum_j a_j^*(1-q_j)P_{ij} - \frac{1}{2}\alpha q_i^2, \tag{D7}$$

and that the equilibrium solves $\frac{\partial \Pi_i}{\partial q_i} = 0$. The derivative of (D7) is given by

$$\frac{\partial \Pi_i}{\partial q_i} = a_i^* - \sum_{j\in V} \frac{\partial a_j^*}{\partial q_i}(1-q_j)P_{ij} - \alpha q_i \tag{D8}$$

Step 1. We prove that Π_i is quasi-concave in q_i. The derivative of (D8) is given by

$$\begin{aligned}\frac{\partial^2 \Pi_i}{\partial q_i^2} &= 2\frac{\partial a_i^*}{\partial q_i} - \sum_{j\in V} \frac{\partial^2 a_j^*}{\partial q_i^2}(1-q_j)P_{ij} - \alpha \\ &= -2D\frac{n^*-1}{\omega n^*} - \alpha < 0,\end{aligned} \tag{D9}$$

where the second equality follows from (16) and $\frac{\partial^2 a_j^*}{\partial q_i^2} = 0$. As the second derivative of the utility of agent i is negative, we conclude that Π_i is actually concave. We are now in the position to apply the result by Debreu, Fan, Glicksberg[24,25,26] who showed that a pure strategy Nash equilibrium exists in the strategic form game of stage 1 when the strategy sets are compact and convex, and the utility of each agent is quasi-concave in the agent's own strategy and continuous in the strategy of other agents.

Step 2. We start by finding the second order derivatives of Π_i. In (D9) we already computed this derivative to q_i. Additionally note that the derivative of (D8) to q_j for $j \neq i$ is given by

$$\begin{aligned}\frac{d^2 \Pi_i}{dq_i dq_j} &= \frac{da_i^*}{dq_j} + \frac{da_j^*}{dq_i}P_{ij} - \sum_{\kappa\in V} \frac{d^2 a_\kappa^*}{dq_i dq_j}(1-q_\kappa)P_{i,\kappa} \\ &= \frac{D}{\omega n^*}(1+P_{ij}),\end{aligned}$$

where $\frac{d^2 a_\kappa^*}{dq_i dq_j} = 0$ is used in the second equality.

Secondly, we determine the number of agents having a positive probability of being attacked, n^*. For any agent i

$$\begin{aligned}\frac{\partial \Pi_i}{\partial q_i}(\{0, q_{-i}\}) &= a_i - \sum_{j\neq i} \frac{\partial a_j}{\partial q_i}[1-q_j]P_{i,j} - \frac{\partial a_i}{\partial q_i} \\ &> a_i - \sum_{j\neq i} \frac{\partial a_j}{\partial q_i} - \frac{\partial a_i}{\partial q_i} \\ &= a_i - \sum_{j\neq i} \frac{\partial a_j}{\partial q_i} = a_i \geq 0.\end{aligned} \tag{D10}$$

This implies that $q_i > 0$: that is, it is not optimal not to investment, since slightly increasing the investment level will result in larger rewards. Now assume that $a_i^* = 0$. By (D7), the rewards of agent i will be

$$\Pi_i = 1 - \sum_{j\neq i} a_j^*(1-q_j)P_{ij} - \frac{1}{2}\alpha q_i^2.$$

Since the equilibrium investments q_i maximize these rewards, we should have $q_i = 0$. But this contradicts our conclusion from (D10). Therefore, our assumption $a_i^* = 0$ was false and we must have $a_i^* > 0$ for all agents i. This implies $n^* = n$, all agents have a positive probability of being attacked.

Combining these results, the negated Jacobian $-\boldsymbol{J}$ with $J_{ij} = \frac{\partial^2 \Pi_i}{\partial q_i \partial q_j}$ becomes

$$-\boldsymbol{J} = \begin{bmatrix} \frac{2n-2}{\omega n} D + \alpha & -\frac{D}{\omega n}(1+P_{12}) & \cdots & -\frac{D}{\omega n}(1+P_{1n}) \\ -\frac{D}{\omega n}(1+P_{21}) & \frac{2n-2}{\omega n} D + \alpha & \cdots & -\frac{D}{\omega n}(1+P_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{D}{\omega n}(1+P_{n1}) & -\frac{D}{\omega n}(1+P_{n2}) & \cdots & \frac{2n-2}{\omega n} D + \alpha. \end{bmatrix} \tag{D11}$$

Next we show that the matrix $-\boldsymbol{J}$ is diagonally dominant.

$$\begin{aligned} \sum_{j \neq i} |-J_{ij}| &= \sum_{j \neq i} \frac{D}{\omega n}(1+P_{ij}) \\ &= \frac{D(n-1)}{\omega n} + \frac{D(D-1)}{\omega n} \\ &\leq \frac{D(n-1)}{\omega n} + \frac{D(n-1)}{\omega n} \\ &= D\frac{2n-2}{\omega n} \ \leq \ |-J_{ii}|, \text{ for all } i. \end{aligned}$$

Because the matrix $-\boldsymbol{J}$ is also symmetric, all principal minors in the negated Jacobian are positive[27]. Because of this, the Nash equilibrium in a symmetric game is unique[28]. As we already concluded that a pure Nash equilibrium always exists, we are able to conclude that this equilibrium is unique and symmetric.

Step 3. Finally, we exhibit the symmetric equilibrium $\mathbf{q} = q\mathbf{1}$. Because of this symmetry, $a_i^* = 1/n$ by Corollary 1. Starting from (D8) we obtain

$$\begin{aligned} \frac{\partial \Pi_i}{\partial q_i} &= \frac{1}{n} - (1-q) \sum_{j \in V} \frac{\partial a_j^*}{\partial q_i} P_{ij} - \alpha q \\ &= \frac{1}{n} + (1-q)\frac{n-1}{\omega n} D - (1-q)\frac{D}{\omega n}(D-1) - \alpha q \\ &= \frac{1}{n} + (1-q)\frac{D}{\omega n}(n-D) - \alpha q. \end{aligned}$$

Since the equilibrium solves $\partial \Pi_i / \partial q_i = 0$, the expression (21) follows immediately.

References

1. Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences* 2014; 80.
2. Varian HR. Managing Online Security Risks. *New York Times* 2000.
3. Acemoglu D, Malekian A, Ozdaglar A. Network security and contagion. *Journal of Economic Theory* 2016; 166: 536-585. doi: https://doi.org/10.1016/j.jet.2016.09.009
4. Lou J, Vorobeychik Y. Equilibrium Analysis of Multi-defender Security Games. In: IJCAI'15. AAAI Press; 2015: 596–602.
5. Pieters J. Dutch Tax Authority also hit in DDoS attack. https://nltimes.nl/2018/01/29/dutch-tax-authority-also-hit-ddos-attack; 2018. [Online; accessed 21-August-2019].
6. Meulen V. dN. Investing in Cybersecurity. *RAND Europe Research Report* 2015.
7. Heal G, Kunreuther H. You Only Die Once: Managing Discrete Interdependent Risks. Working Paper 9885, National Bureau of Economic Research; 2003
8. Li M, Koutsopoulos I, Poovendran R. Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks. In: ; 2007: 1307-1315

9. Amin S, Schwartz GA, Sastry SS. Security of interdependent and identical networked control systems. *Automatica* 2013; 49(1): 186-192. doi: https://doi.org/10.1016/j.automatica.2012.09.007

10. Zhu Q, Basar T. Game-Theoretic Methods for Robustness, Security, and Resilience of Cyberphysical Control Systems: Games-in-Games Principle for Optimal Cross-Layer Resilient Control Systems. *IEEE Control Systems* 2015; 35(1): 46-65. doi: 10.1109/MCS.2014.2364710

11. Yuan Y, Yuan H, Guo L, Yang H, Sun S. Resilient Control of Networked Control System Under DoS Attacks: A Unified Game Approach. *IEEE Transactions on Industrial Informatics* 2016; 12(5): 1786-1794. doi: 10.1109/TII.2016.2542208

12. Gupta A, Langbort C, Basar T. Dynamic Games With Asymmetric Information and Resource Constrained Players With Applications to Security of Cyberphysical Systems. *IEEE Transactions on Control of Network Systems* 2017; 4(1): 71-81. doi: 10.1109/TCNS.2016.2584183

13. Chan H, Ceyko M, Ortiz L. Interdependent Defense Games: Modeling Interdependent Security Under Deliberate Attacks. In: UAI'12. AUAI Press; 2012; Arlington, Virginia, United States: 152–162.

14. Zhu Q, Tembine H, Basar T. Network Security Configurations: A Nonzero-Sum Stochastic Game Approach. In: ; 2010: 1059-1064.

15. Anderson R, Moore T. The Economics of Information Security. *Science* 2006; 314(5799): 610–613. doi: 10.1126/science.1130992

16. Manshaei MH, Zhu Q, Alpcan T, Basar T, Hubaux JP. Game theory meets network security and privacy. *ACM Computing Surveys* 2013; 45(3): 25:1-25:39.

17. Laszka A, Felegyhazi M, Buttyan L. A Survey of Interdependent Information Security Games. *ACM Computing Surveys* 2014; 47(2): 23:1–23:38. doi: 10.1145/2635673

18. He X, Dai H. *Dynamic Games for Network Security*. Springer . 2018.

19. Lelarge M, Bolot J. Economic Incentives to Increase Security in the Internet: The Case for Insurance. In: ; 2009: 1494-1502

20. Bachrach Y, Draief M, Goyal S. Contagion and observability in security domains. In: ; 2013: 1364-1371

21. Peters H. *Game Theory: A Multi-Leveled Approach*. Springer Texts in Business and EconomicsSpringer . 2016.

22. Bier V, Oliveros S, Samuelson L. Choosing What to Protect: Strategic Defensive Allocation against an Unknown Attacker. *Journal of Public Economic Theory* 2007; 9(4): 563–587. doi: 10.1111/j.1467-9779.2007.00320.x

23. Johnson B, Grossklags J, Christin N, Chuang J. Nash Equilibria for Weakest Target Security Games with Heterogeneous Agents. In: Jain R, Kannan R., eds. *Game Theory for Networks*Springer Berlin Heidelberg; 2012: 444-458.

24. Debreu G. A Social Equilibrium Existence Theorem. *Proceedings of the National Academy of Sciences* 1952; 38(10): 886–893. doi: 10.1073/pnas.38.10.886

25. Fan K. Fixed-point and Minimax Theorems in Locally Convex Topological Linear Spaces. *Proceedings of the National Academy of Sciences* 1952; 38(2): 121–126.

26. Glicksberg IL. A Further Generalization of the Kakutani Fixed Point Theorem, with Application to Nash Equilibrium Points. *Proceedings of the American Mathematical Society* 1952; 3(1): 170-174.

27. Bapat RB, Raghavan TES. *Nonnegative Matrices and Applications*. Encyclopedia of Mathematics and its Applicationsons Cambridge University Press . 1997

28. Gale D, Nikaido H. The Jacobian matrix and global univalence of mappings. *Mathematische Annalen* 1965; 159(2): 81–93. doi: 10.1007/BF01360282

AUTHOR BIOGRAPHY

Bram de Witte received his M.Sc (in applied mathematics) from the University of Twente in 2015. From 2015 on he worked in financial markets respectively at an insurance company and at the Dutch authority for the financial markets. His research interest lies at actuarial science and financial mathematics.

Paolo Frasca received the Ph.D. degree in Mathematics for Engineering Sciences from Politecnico di Torino, Torino, Italy, in 2009. Between 2008 and 2013, he has held research and visiting positions at the University of California, Santa Barbara (USA), at the IAC-CNR (Rome, Italy), at the University of Salerno (Italy), and at the Politecnico di Torino. From 2013 to 2016, he has been an Assistant Professor at the University of Twente in Enschede, the Netherlands. Since October 2016 he is a CNRS Researcher with GIPSA-lab, Grenoble, France. His research interests are in the theory of network systems and cyber-physical systems, with main applications to infrastructural and social networks. Dr. Frasca has been a Visiting Professor at the LAAS, Toulouse, France, in 2016 and at the University of Cagliari, Italy, in 2017. He has served or is serving as Associate Editor in the Conference Editorial Boards of the IEEE Control Systems Society and of the European Control Association (EUCA) and for the International Journal of Robust and Nonlinear Control, the Asian Journal of Control, and the IEEE Control Systems Letters.

Bastiaan Overvest received his Ph.D. degree in Economics from the University of Groningen, the Netherlands, in 2009 for a thesis on game-theoretic properties of price collusion and market sharing agreements. Between 2008 and 2014, he served as case handler and researcher at the Netherlands Competition Authority, NMa. In 2014 he moved to the Netherlands Bureau for Economic Policy Analysis where he conducted research on innovation, cybersecurity and digitalization. In 2018 he was appointed as program leader for Innovation and Science. His research interests are in the theory and empirics of competition, platforms, digitization.

Judith Timmer received her M.Sc. (in econometrics) and Ph.D. degrees from the Tilburg University, Tilburg, the Netherlands. Currently she is assistant professor in the Mathematics of Operations Research group at the University of Twente, Enschede, the Netherlands. Her research focuses on improving the performance of queueing networks, communication networks and inventory systems with game theory.